PLAN DU SOUS SAVOIR S36

A. INTRODUCTION A LA SUPERVISION DES RESEAUX INFORMATIQUES

1. Définition de la supervision d'un réseau.

Dans un réseau informatique, que veut dire "superviser" ?
Il s'agit de regarder TOUT sauf l'information.

Super = au dessus
Viser = regarder
Superviser = Regarder au dessus ≠ regarder l'information= espionner

Exemple

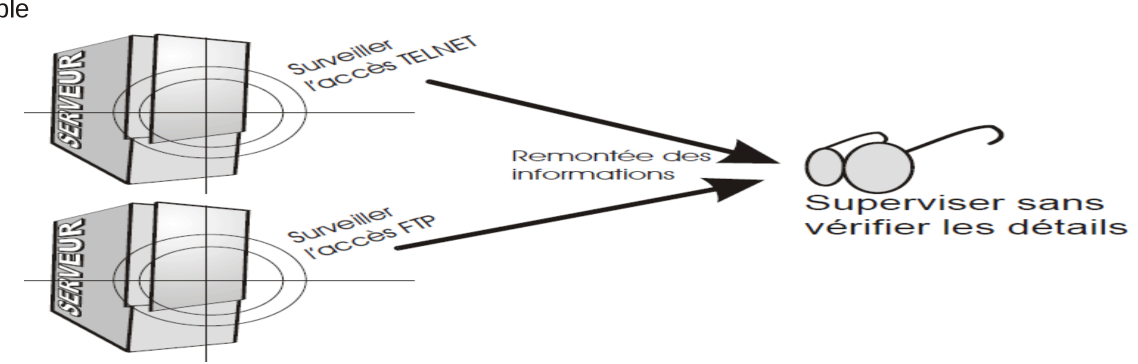


Attention : superviser ne vous autorise pas à regarder l'information.

2. Problématiques de la supervision et de la surveillance.

La surveillance = regarder quelque chose de précis. Par exemple : surveiller la porte d'entrée (rien d'autre).
Superviser c'est, en réalité, surveiller plusieurs organes.

Exemple



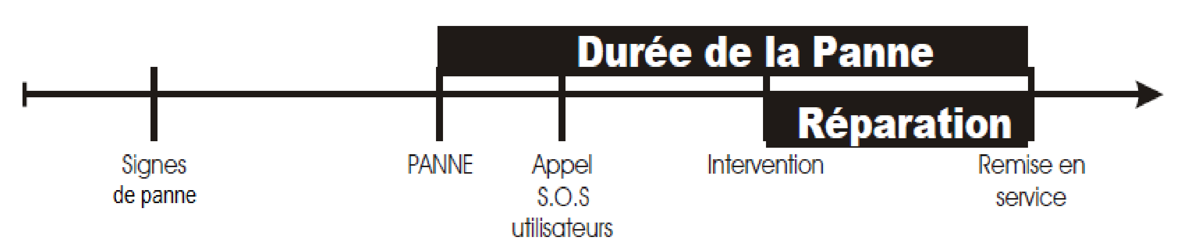
Je supervise dans le but d'être informé sur l'état de mon réseau ou de mes applications…
Si je ne supervise pas :

- Je peux être piraté sans le savoir
- Mes serveurs peuvent être fatigués
- Mes performances peuvent tomber
- Les utilisateurs préviennent en cas de panne – je perds toute crédibilité
- Ma Direction se lasse : "l'informatique est toujours en panne" …

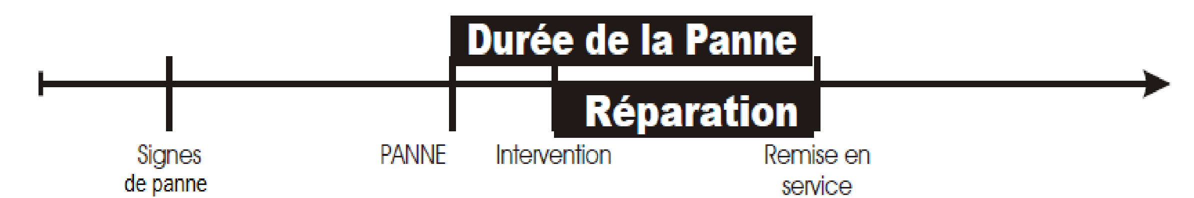
Je supervise pour ma tranquillité et ma crédibilité donc j'ai besoin de la supervision pour mon image.

3. Pourquoi ne pas attendre la panne tout simplement ?

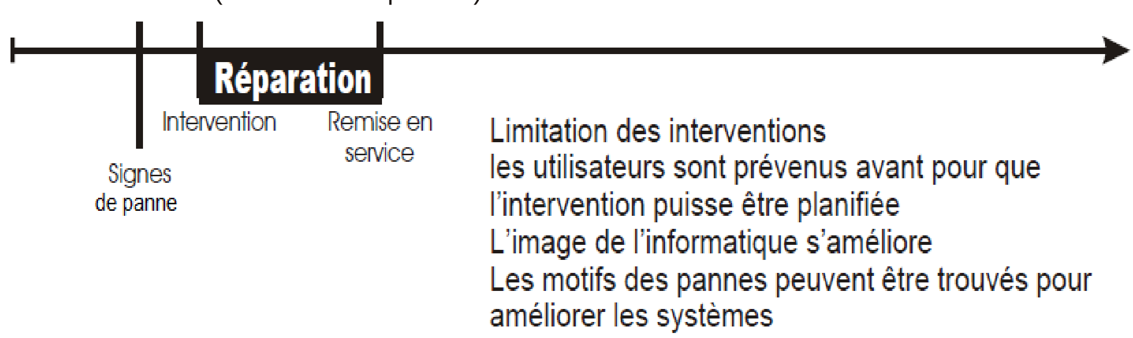
Si j'attends la panne



Si je supervise mal (post-panne)



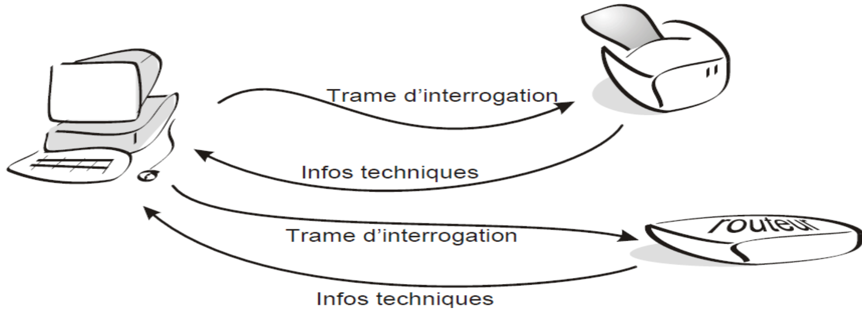
Je supervise correctement (tolérance aux pannes)



B . Protocole de supervision SNMP

1. Introduction

Il existe plein de moyens pour superviser automatiquement les organes d'un réseau. L'un des moyens actuels standard est le protocole SNMP *(Simple Network Management Protocol),* avec ce moyen on peut connaître les informations internes d'un routeur, d'une imprimante, de certains Switchs et de serveurs …



Le protocole SNMP permet de :

- Connaître l'état d'un appareil => en lui envoyant une question
- Avoir une vue sur les données locales => nb paquets passés …
- Configurer => en lui donnant un ordre, l'élément peut changer sa configuration
- Alerter => dans ce protocole, un port est réservé aux alertes

2. Origine du protocole SNMP

SNMP (Simple Network Management Protocol) a été adopté comme norme pour les réseaux TCP/IP en 1989. Ce protocole désigne un ensemble de normes d'administration, notamment :

- Un protocole de communication
- Une spécification de structure de base de données
- Un ensemble d'objets de données

Très populaire et présent dans la plupart des réseaux d'entreprise, SNMP connu une mise à niveau (SNMPv2c) en 1993, améliorant entre autre la structure des informations d'administration, l'authentification ainsi que le protocole lui-même. SNMP évolue pour en arriver à la version 3 (SNMPv3) qui prend en charge l'authentification et le cryptage des communications tout en restant rétro compatible.

3. Fonctionnement

SNMP est un protocole de la couche application conçu pour faciliter l'échange d'informations d'administration entre les équipements réseaux. On peut par exemple l'utiliser pour accéder à des données d'informations d'administrations tels que le nombre de paquets en sortie sur l'interface WAN d'un routeur, le nombre de connexions TCP ouvertes ou même la quantité d'erreur détectées sur cette même interface.

La quantité d'informations accessibles et récupérables est très nombreuse et détaillée. SNMP est un protocole simple, mais ses fonctions sont suffisamment efficaces pour gérer les problèmes liés à l'administration des réseaux hétérogènes. Le modèle organisationnel de l'administration réseau SNMP comporte quatre éléments :

- La station de gestion du réseau (NMS : Network Management System)
- Les agents de supervision (Agent SNMP)
- La base d'information de management (MIB : Management Information Base)
- Le protocole de gestion réseau.

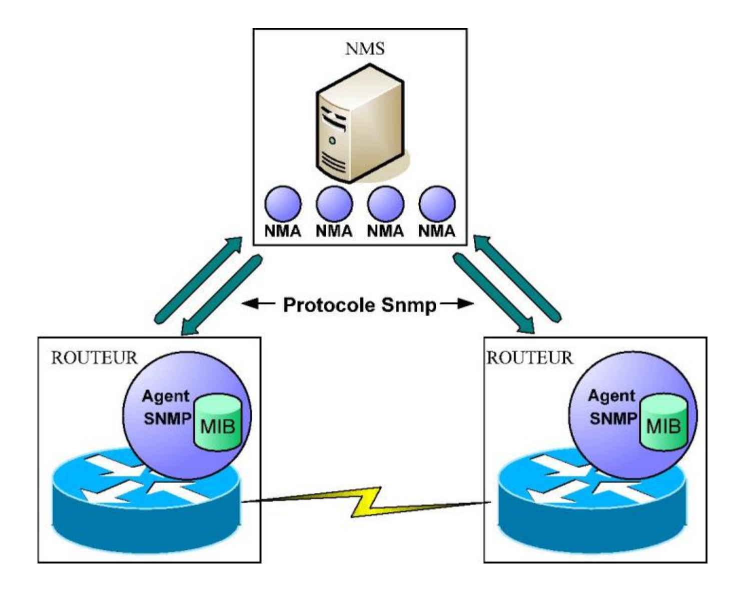


Figure 2-Fonctionnement de SNMP

La NMS est généralement une station de travail autonome. Elle se compose d'un ensemble de logiciels appelé NMA.
Ceux-ci intègrent une interface utilisateur permettant aux administrateurs de superviser le réseau en récupérant des informations sur les agents SNMP. Ceux-ci sont situés sur les différents équipements réseaux (routeur, pont, commutateur, répéteur, serveur d'application).

Un agent SNMP peut répondre à une requête d'exécution d'action de la part de la NMS. Il peut également remonter des informations utiles, non sollicitées par la NMS, telles que la perte de connectivité entre deux routeurs, ou un disfonctionnement du service de messagerie de l'entreprise.

Un agent SNMP peut effectuer un suivi de ces éléments :

- Le nombre et l'état de ses circuits virtuels.
- Le nombre de certains types de messages d'erreur reçus.
- Le nombre d'octets et de paquets entrant et sortant de l'équipement.
- La longueur maximale de la file d'attente de sortie pour les routeurs et autres équipements inter réseaux.
- Les messages de broadcast envoyés et reçus.
- L'état d'activation des interfaces réseau.

Afin de permettre à une NMS de dialoguer avec un agent SNMP, le protocole définit une chaîne de caractère : « l'identifiant de communauté ». Les échanges ne sont possibles qu'entre agents et NMA d'une même communauté SNMP.

- Cette forme très basique de vérification reste une simple identification implémentée dans le protocole SNMP (SNMPv1).Ceci représentant une faille de sécurité de taille (cet identifiant transitant en clair).

- La version 2 de SNMP a bénéficié de l'implémentation de mécanismes d'authentification et d'intégrité (chiffrement symétrique à clé privée utilisant l'algorithme HMAC-MD5-96). Cette version pose des problèmes de rétro compatibilité.

- La version 3 a été conçue pour parer à ces problèmes. SNMPv3 permet donc une sécurité accrue ainsi qu'une rétro compatibilité.

A un identifiant de communauté, peut être affecté des permissions en lecture seulement ou en lecture/écriture sur les objets.
La communauté par défaut pour la lecture seule est « public », et « private » pour l'accès en lecture et écriture.

Version	Authentification	Confidentialité	Cryptage	Fonctionnement
SNMPv1	Non	Non	Non	Identification assurée par l'appartenance à la communauté SNMP
SNMPv2c	Oui	Oui	Oui	Authentification par chiffrement symétrique Problème de rétro compatibilité
SNMPv3	Oui	Oui	Oui	Authentification par chiffrement symétrique Rétro compatible

Tableau 1- Différences SNMPv1, SNMPv2c et SNMPv3

SNMP est un protocole de la couche application qui utilise les ports UDP 161 (NMS) et 162 (Agent). Il fonctionne selon un système d'échange de messages.

Ces derniers peuvent être de types :

- **Get** : Récupération de la valeur d'un objet de la MIB à partir de l'agent, nécessite au moins les droits en lecture.
- **Set** : Affecter une valeur à l'un des objets MIB grâce a l'agent, nécessite les droits en lecture et écriture.
- **Trap** : Utilisé par l'agent afin de signaler des informations jugées «importantes» à la NMS.

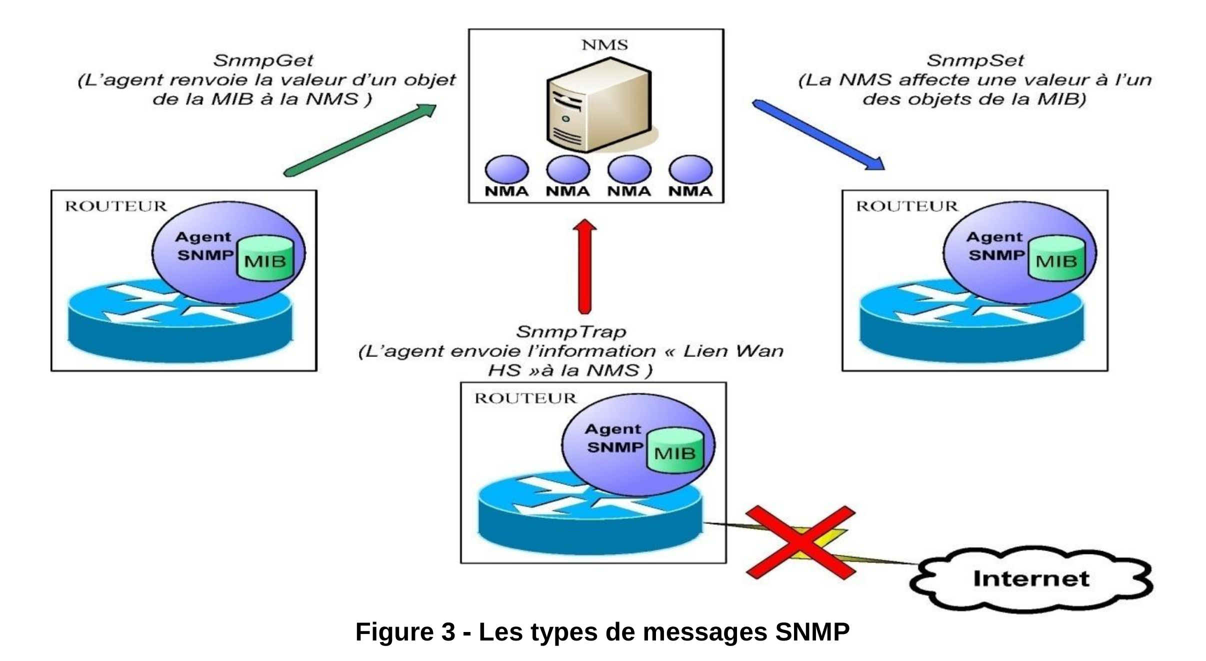


Figure 3 - Les types de messages SNMP

4. MIB

La MIB est organisée en arborescence définie par la norme SMI (Structure of Management Information). SMI spécifie également les types de données utilisés pour stocker un objet (entier, chaîne de caractère), la manière dont ces objets sont nommés etc. Chaque élément final de la MIB représente un attribut de l'équipement réseau concerné.

C'est un référentiel contenant une somme considérable d'informations concernant l'équipement. Il existe des MIB standards et propriétaires :

La MIB SMI d'origine est composée de 8 groupes et de 114 objets. Nous en sommes actuellement à la version 2 de la MIB aussi appelée MIB-II.

Les MIB propriétaires sont propres aux équipements du constructeur.

Ci-dessous, un exemple de MIB-II :

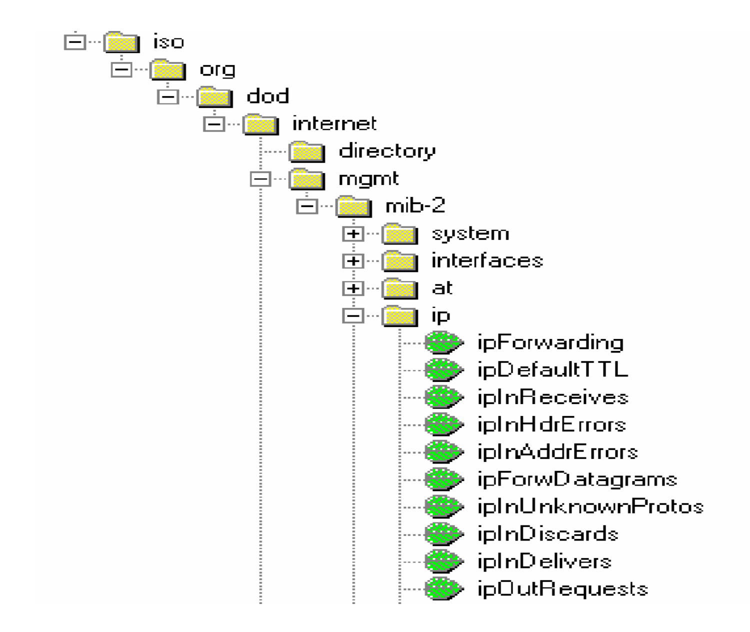


Figure 4 - Représentation logicielle d'une MIB

Chaque feuille de la MIB est identifiée par une OID (Object Identifier).
Une OID est une information constituée de valeurs décimales pointées. (Exemple : 1.3.6.1.2.1.4.3).
Chaque valeur décimale de l'OID identifie l'une des branches de la MIB.
Exemple pour l'objet « **ipInReceives** »:
iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ip(4).ipInReceives(3)
Le schéma ci-dessous présente les différents groupes de la MIB ainsi que leurs OID:

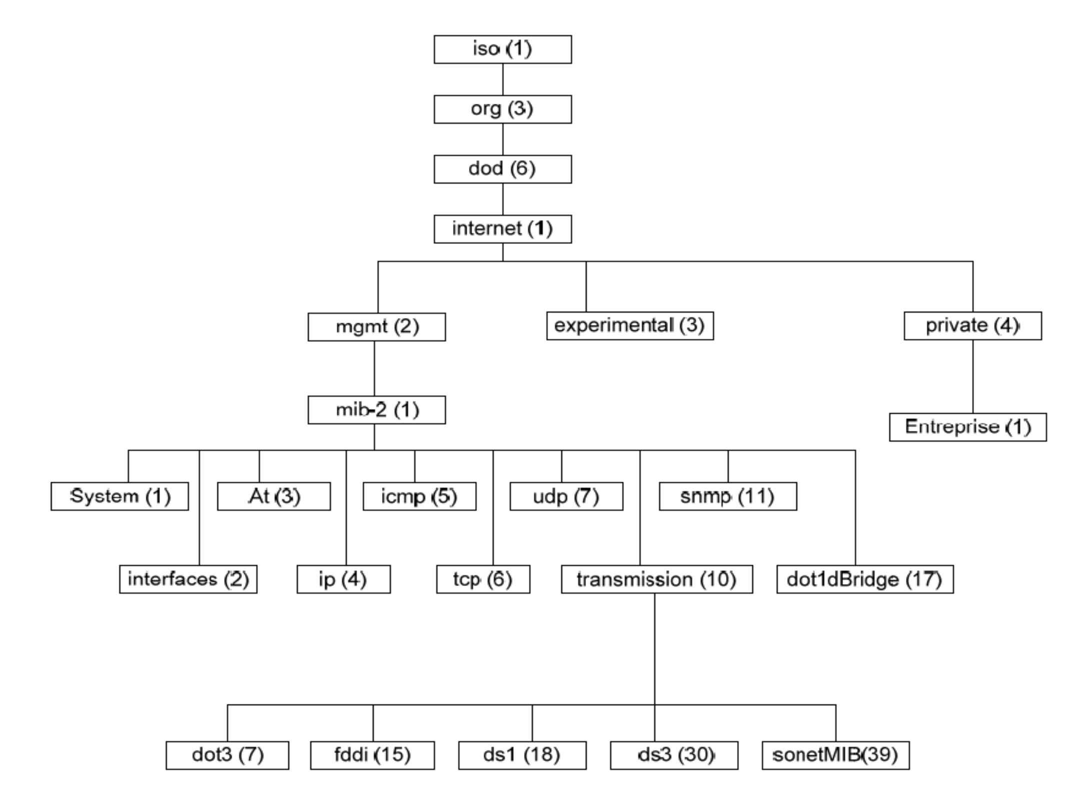


Figure 5 - Représentation des groupes de la MIB et de leur OID

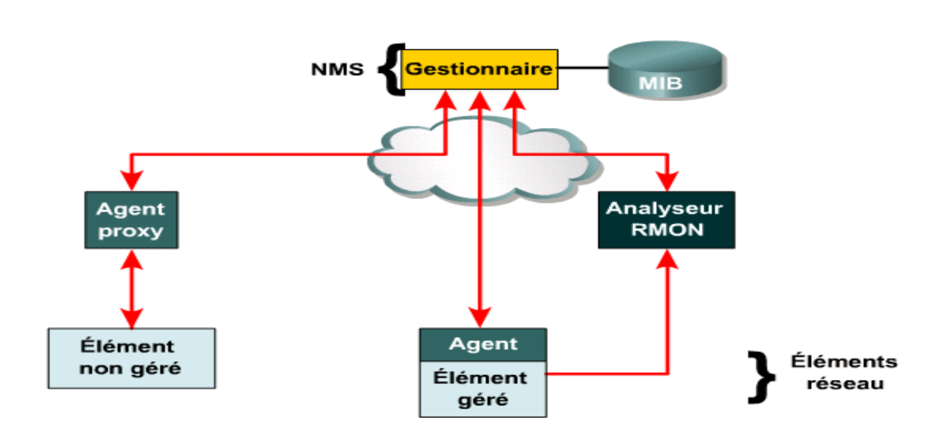
5. Configuration

Voici les commandes de configuration nécessaires à la communication entre les équipements réseaux et la NMS :

- **snmp-server community {communauté} ro**
  - Mode de configuration globale
  - Autorise l'accès en lecture seule à la communauté spécifiée
- **snmp-server community {communauté} rw**
  - Mode de configuration globale
  - Autorise l'accès en lecture et écriture à la communauté spécifiée
- **snmp-server location {emplacement}**
  - Mode de configuration globale
  - Configure la description de l'emplacement du routeur
- **snmp-server contact {chaîne de caractère}**
  - Mode de configuration globale
  - Configure les informations relatives aux personnes à contacter si besoin est
- **snmp-server host {IP de la NMS} {communauté}**
  - Mode de configuration globale
  - Spécifie une NMS qui recevra les Traps SNMP
- **snmp-server enable traps snmp [authentication][linkup][linkdown][coldstart] [warmstart]**
  - Mode de configuration globale
  - Spécifie le(s) événement(s) qui déclencheront l'envoie des traps

6. RMON

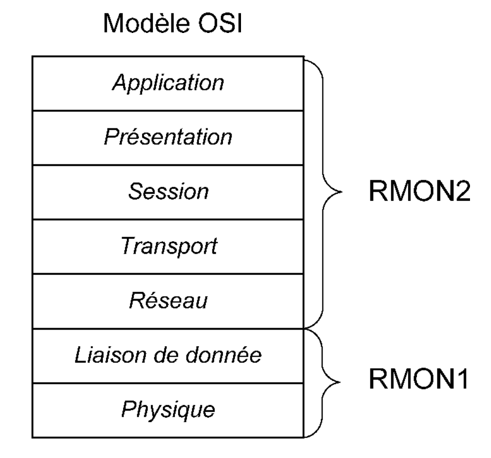
RMON (Remote Monitoring) définit une MIB de surveillance qui complète MIB-II. Cette MIB contient des informations de statistiques obtenues en analysant chaque trame d'un segment du réseau. Pour se faire, des dispositifs de surveillance matérielle (sonde RMON) sont placés sur les segments à surveiller. Ces dispositifs permettent de créer des alarmes définies par l'utilisateur, mais surtout de rassembler une multitude de statistiques vitales grâce à l'analyse approfondie de chaque trame d'un segment.



Avec RMON, l'administrateur peut obtenir des informations relatives à la globalité d'un segment LAN (pourcentage de collisions sur le segment, stations émettant le plus de broadcast etc....).

RMON n'a pas nécessité la modification du protocole SNMP, il n'a suffit pour intégrer RMON que de rajouter des entités dans la MIB. Il existe en deux versions :

RMON1 – Fonctionnant au niveau des couches 1 et 2 du modèle OSI.
RMON2 – Fonctionnant au niveau des couches 3 à 7 du modèle OSI.



7. Syslog

Fonctionnement

Syslog est un utilitaire de consignation d'évènements Cisco basé sur l'utilitaire Syslog d'Unix. A l'origine, Syslog avait été développé pour le logiciel Sendmail uniquement. Mais l'utilité de ce dernier était telle que beaucoup d'autres applications se sont mises à l'utiliser. Syslog fonctionne sur un modèle client - serveur.

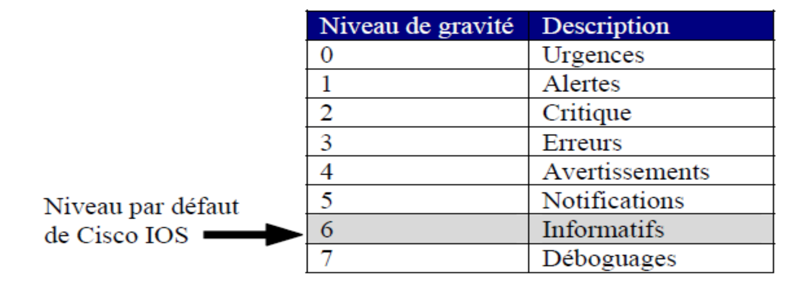
Le port utilisé sur le serveur est le port UDP/514 et la taille des messages ne peut excéder 1024 octets. En 2001, les spécifications de Syslog ont été définies dans la RFC 3164.

Sur un routeur ou commutateur Cisco, les évènements Syslog peuvent être envoyés sur une NMS. Les messages envoyés seront alors de type « non sollicités » (Traps).

Chaque message syslog est horodaté, contient un niveau de gravité ainsi qu'un message de consignation. Ces messages sont parfois la seule manière de résoudre un problème sur les équipements. Il existe 8 niveaux de gravité dans les Traps Syslog (0 à 7). Le niveau 0 étant le plus critique (7 le moins).

Un équipement réseau n'enverra au serveur Syslog que des messages dont la gravité est supérieure (inférieure en chiffre) au seuil défini.

Par défaut, le niveau de gravité est à 6 sur les IOS Cisco. On aura donc tous les messages disponibles excepté ceux de débogage.



Niveau de gravité	Description
0	Urgences
1	Alertes
2	Critique
3	Erreurs
4	Avertissements
5	Notifications
6	Informatifs
7	Déboguages

Par défaut, Cisco IOS adopte le niveau de gravité 6. Ce paramètre est configurable.

Configuration

Pour que la NMS puisse recevoir les traps Syslog d'un équipement, il faut qu'une application serveur Syslog (CiscoWorks2000, Kiwi Syslog...) soit configurée sur celle-ci.

Il faut également configurer le routeur pour l'envoi des évènements sur la NMS. Ci-dessous, les différentes commandes de configurations nécessaires sur un routeur 2620xm :

- **logging on**
  - Mode de configuration globale
  - Active la consignation des évènements

- **logging {nom d'hôte} | {adresse IP de la station}**
  - Mode de configuration globale
  - Spécifie au routeur la station NMS recevant les traps Syslog

- **logging trap {debugging | informational | notification | warnings | errors | critical | alerts | emergencies}**
  - Mode de configuration globale
  - Configure le niveau de gravité (optionnel)

- **service timestamps log datetime**
  - Mode de configuration globale
  - Horodate les messages syslog (optionnel)

C. Mise en œuvre de SNMP

Examen des solutions techniques de supervision disponibles utilisant SNMP :

Pour répondre au mieux à ce problème, nous allons procéder à une analyse des principales solutions de supervision utilisés. Les solutions comparées sont toutes basées sur Linux comprenant aucun coût d'acquisition. Le coût de la solution « Microsoft System Center » est trop important en termes d'acquisition et de support.

Les solutions	Points forts	Points faibles
Centreon	- Robustesse et renommée de nagios - Peut être séparé du serveur Nagios et tourner tout seul sur un autre serveur - solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau	- L'interface peut paraître complexe car il existe beaucoup d'options, de vues - Interface lourde
EON Eyes Of Network	- Repose sur nagios - Communauté nagios importante et active - Plugin installé pour interfacer cacti, ntop, - solution « tout en un »	- Les outils nagios, nagvis, cacti tributaire des Patchs de LILAC (Interface de EON) - Temps de configuration de l'outil importante (basé sur plusieurs outils à comprendre)
Nagios	Une solution complète Beaucoup de documentation sur le net Reconnu des entreprises, grande communauté	Interface non ergonomique et peu intuitive. Configuration fastidieuse via beaucoup de fichiers. Pour avoir toute les fonctionnalités il faut installer des plugins, de base c'est assez limité.
ZABBIX	- Agent zabbix propriétaire - Cartographie propre à zabbix (moins performante que nagvis) - Graphe (moins performant que cacti)	- Solution jeune qui date de 2010 - Communauté peu importante
big brother PROFESSIONAL EDITION	- changement de couleur de l'interface en fonction de l'état actuel des machines. - interface claire et simple	- Pas de graphe possible - Pas d'accès avec ACL
openNMS®	- Discovery snmp performant - Diverses graphes et rapide d'accès	- Orienté réseau - Fonctionnalités réduites - Difficulté de réunir plusieurs graphes.